What Is Claimed Is:

1. A method for remotely configuring a device across a network, comprising:

receiving configuration information at the device from a remote system across the network;

encrypting the configuration information using a device key, wherein the device key is locally stored at the device and is different from keys associated with other devices; and

configuring the device by storing the encrypted configuration information in a non-volatile configuration store associated with the device;

whereby the encrypted configuration information contained in the non-volatile configuration store cannot be used with another device.

2. The method of claim 1, wherein receiving the configuration information involves using a secret key, which is locally stored at the device, to decrypt the configuration information received from the remote system.

3. The method of claim 1, wherein receiving the configuration information involves using a public key of the remote system to validate that the configuration information was digitally signed by a corresponding private key belonging to the remote system.

4. The method of claim 1, wherein the device key is stored in one-time programmable memory within the device that can be programmed only once and cannot be reprogrammed.

5. The method of claim 1, wherein the device uses the configuration information to control access to a stream of content in order to facilitate subscriber management.

6. The method of claim 5, wherein the configuration information includes either a fixed key or a variable key for decompression and/or decryption of the stream of content.

7. The method of claim 1, wherein the device includes one of:
a computer;
a personal digital assistant;
a network interface;
a cable television interface;
a satellite television interface; and
a network router.

8. The method of claim 1, wherein the network includes one of:
a local area network;
a wide area network; and
a wireless network.

9. The method of claim 1, wherein configuring the device can involve enabling or disabling the device.

10. The method of claim 1, wherein the device is embodied in an integrated circuit.

11. An apparatus that facilitates remotely configuring a device across a network, comprising:

an interface, at the device, that is configured to receive configuration information from a remote system across the network;

an encryption mechanism that is configured to encrypt the configuration information using a device key, wherein the device key is locally stored at the device and is different from keys associated with other devices; and

a configuration mechanism that is configured to store the encrypted configuration information in a non-volatile configuration store associated with the device;

whereby the encrypted configuration information contained in the non-volatile configuration store cannot be used with another device.

12. The apparatus of claim 11, further comprising a decryption mechanism that is configured to use a secret key, which is locally stored at the device, to decrypt the configuration information received from the remote system through the interface.

13. The apparatus of claim 11, further comprising a validation mechanism that is configured to use a public key of the remote system to validate that the configuration information was digitally signed by a corresponding private key belonging to the remote system.

14. The apparatus of claim 11, further comprising a one-time programmable memory within the device for storing the device key;

wherein the one-time programmable memory can be programmed only once and cannot be reprogrammed.

15. The apparatus of claim 11, further comprising a content screening mechanism that is configured to use the configuration information to control access to a stream of content in order to facilitate subscriber management.

16. The apparatus of claim 15, wherein the configuration information includes either a fixed key or a variable key for decompression and/or decryption of the stream of content.

17. The apparatus of claim 11, wherein the device includes one of:
a computer;
a personal digital assistant;
a network interface;
a cable television interface;
a satellite television interface; and
a network router.

18. The apparatus of claim 11, wherein the network includes one of:
a local area network;
a wide area network; and
a wireless network.

19. The apparatus of claim 11, wherein the configuration mechanism can enable and/or disable the device.

20. The apparatus of claim 11, further comprising an integrated circuit upon which the device is embodied.

21. The apparatus of claim 11, wherein the interface is configured to support one-way communication from the remote system to the device.

22. The apparatus of claim 11, further comprising a local interface on the device for communicating with local resources;

wherein the local interface is insulated from the configuration information stored in the non-volatile configuration store, so that it is impossible to access the configuration information through the local interface.

23. An apparatus that facilitates remotely configuring a device across a network, comprising:

an interface, at the device, that is configured to receive configuration information from a remote system across the network;

a decryption mechanism that is configured to use a secret key, which is locally stored at the device, to decrypt the configuration information received from the remote system through the interface;

an encryption mechanism that is configured to encrypt the configuration information using a device key, wherein the device key is locally stored at the device and is different from keys associated with other devices; and

a configuration mechanism that is configured to store the encrypted configuration information in a non-volatile configuration store associated with the device; and

a one-time programmable memory within the device for storing the device key and the secret key, wherein the one-time programmable memory can be programmed only once and cannot be reprogrammed;

whereby the encrypted configuration information contained in the non-volatile configuration store cannot be used with another device.

24. The apparatus of claim 23, further comprising a content screening mechanism that is configured to use the configuration information to control access to a stream of content in order to facilitate subscriber management.

25. The apparatus of claim 23, further comprising a validation mechanism that is configured to use a public key of the remote system to validate that the configuration information was digitally signed by a corresponding private key belonging to the remote system.